Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Primitive Groups with a Determination of the Primitive Groups of Degree 20.

By Elizabeth R. Bennett.

Introduction.

Substitution groups were first considered in connection with the solution of algebraic equations. The earliest work that devotes considerable attention to these groups (Ruffini, *Teoria generale delle equazioni*, Bologna, 1799) divides the substitution groups, or permutations, as Ruffini calls them, into two main classes, viz., the cyclic and non-cyclic permutations. The non-cyclic permutations are again divided into permutations of the first, second, and third kind, which correspond to what are now known as intransitive, imprimitive, and primitive groups.

The primitive group notion was emphasized later by Galois, who defined primitive groups in connection with primitive equations[*] and who was the first to show the close relation which exists between the theory of substitution groups and the solution of algebraic equations. From his time mathematicians have recognized the fact that the determination of all the substitution groups of a given degree is a fundamental problem of algebra. Since the determination of intransitive groups is based on a knowledge of the transitive groups of lower degree and the determination of imprimitive groups requires a knowledge of primitive groups of lower degree, it is evident that the determination of the primitive groups of different degrees is important for the solution of this fundamental problem. Numerous theorems have been published which aid in this determination, and the enumeration of all the primitive groups of a given degree has been carried through degree 19.[†]

---

[*] Galois, *Œuvres publiés par E. Picard*, Paris, 1897, pp. 11, 53

[†] The possible primitive groups of degree 19 are mentioned by Jordan, Paris *Comptes Rendus*, Vol. LXXIX (1874), p. 1150. Extensive references as regards the primitive groups of lower degree are given in the *Encyclopédie des Sciences Mathématique*, Vol. I, p. 564.

The first part of the present paper contains a number of theorems concerning the determination of simply transitive primitive groups. In Part II the primitive groups of degree 20 are determined, while in Part III certain primitive groups whose maximal subgroup contains a transitive constituent of prime order are considered.

PART I.

Simple Transitive Primitive Groups. General Theorems.

Let G represent a primitive group of degree n and let G_1 represent its maximal subgroup of degree $n-1$. When G is simply transitive, G_1 is intransitive and must contain certain transitive constituents. The determination of all the simply transitive primitive groups of a given degree n, therefore, requires the determination of the intransitive groups of degree $n-1$ which can be maximal subgroups of a primitive group. It is important to know what groups may occur in G_1 as transitive constituents and what relations, if any, must exist between the degrees or between the orders of such transitive constituents. Various theorems which aid either directly or indirectly in the determination of these transitive constituents have been proved by Jordan,[*] Miller,[†] and Rietz.[‡]

In the present paper extensive use has been made of the following theorem and corollary with respect to the transitive constituents of G_1:

THEOREM. If a transitive constituent of G_1 is of a prime order, the order of G_1 is the same prime number, and G is of class $n-1$.

COROLLARY. If G_1 contains a constituent of degree 2, its order is 2, and the degree of G is a prime number.[§]

The corollary, in particular, has suggested the consideration of what additional transitive constituents G_1 must contain when it contains either a transitive constituent of degree 3 or a transitive constituent of degree 4. The results of these considerations are stated in Theorems VII to X.

Certain conditions regarding the transitive constituents which must occur in G_1 are obtained by considering a subgroup K of G_1 which will now be defined. Suppose one of the transitive constituents M of G_1 is a non-regular group of degree m and consider the isomorphism that exists between this group and the group formed from all the other transitive constituents of G_1. The invariant subgroup of G_1 corresponding to identity in the transitive constituent of degree m will be denoted by H and the subgroup composed of all the substitutions leaving a letter of the transitive constituent of degree m fixed will be denoted by K.

---

[*] Jordan, *Traité des Substitutions*, p. 284.

[†] Miller, *Proc. London Math. Soc.*, Vol. XXVIII, pp. 535, 536.

[‡] Rietz, AMERICAN JOURNAL OF MATHEMATICS, Vol. XXVI, pp. 5, 6.

[§] Miller, *Proc. London Math. Soc.*, Vol. XXVIII, p. 536.

In Theorems I to VI inclusive it is assumed that H is of degree $n - m - 1$ and that G_1 contains a transitive constituent M of degree m, but no other transitive constituent whose degree divides m.

THEOREM I. *If the subgroup which is both in K and also in a transitive constituent of degree m_1 of G_1 is transitive, K must contain another transitive constituent of degree m_1 which is not a transitive constituent of G_1 and which is similar to the one previously known to be in K.*

Since K leaves at least one letter of G_1 fixed, it must occur in some conjugate of G_1, as G_1'. The group G_1' may then be considered with respect to the isomorphism which exists between its transitive constituent M' of degree m and the group formed from all the other transitive constituents of G_1'. Since K is composed of all the substitutions leaving a letter of the transitive constituent of degree m fixed, the order of K is one m-th the order of G_1 and, therefore, its order must be one m-th the order of G_1'. Moreover, since the subgroup K leaves a letter of the transitive constituent M of G_1 fixed, when it occurs in G_1' it must also leave a letter of some transitive constituent of G_1' fixed. However, none of the transitive constituents of G_1' except M' have degrees which divide m. Therefore, K could not be contained in a subgroup composed of all the substitutions leaving a letter of a transitive constituent of G_1' fixed, M' excepted, for the order of K would not divide the order of such a subgroup. The subgroup K also could not leave fixed all the letters of a transitive constituent of G_1', for in G_1 K contained letters from all the transitive constituents of G_1. The subgroup K in G_1' must then be composed of all the substitutions leaving a letter of the transitive constituent M' of degree m fixed and must occupy in G_1' a place similar to the one which it occupied in G_1. The transitive constituent m_1 in G_1' cannot have exactly the same letters as in G_1, for if it had this property, G_1 and G_1' would generate an intransitive group. This is impossible since G_1 is a maximal subgroup of G. It is evident that when the subgroup of the transitive constituent of degree m_1 in K is transitive, the letters cannot be partly different from what they were in G_1. Therefore, all the letters of the transitive constituent of degree m_1 in G_1' must be entirely different from what they were in G_1, and K must contain another transitive constituent of degree m_1 which is similar to the one already known to be in it. Since G_1 and G_1' generate G, this additional transitive constituent of degree m_1 in K cannot be a transitive constituent of G_1.

THEOREM II. *If the subgroup which is both in K and also in a transitive constituent of degree m_1 of G_1 is intransitive, then K must contain a transitive constituent similar to one of the transitive constituents occurring in this intransitive subgroup.*

Since K leaves at least one letter of G_1 fixed, it must occur in some conjugate of G_1, as G_1'. When G_1' is considered with respect to the isomorphism which exists between its transitive constituent M' of degree m and the group formed from all the other transitive constituents of G_1', it may be shown as in Theorem I that K occupies in G_1' a place similar to the one which it occupied in G_1. The subgroup which is both in K and also in a transitive constituent of degree m_1 of G_1' is intransitive and will contain in K certain transitive constituents of the same degree. At least one of these must be entirely different from any such constituent occurring in the intransitive subgroup of the constituent of degree m_1 of G_1 which is in K. If such were not the case, G_1 and G_1' would again generate an intransitive group. Therefore, K must contain a transitive constituent similar to one occurring in the subgroup of the group of degree m_1 which is in K and entirely different from it.

If in place of the transitive constituent of degree m_1 in G_1, the transitive constituent M of degree m is considered, a theorem with respect to the subgroup of M composed of all the substitutions leaving a letter of this transitive constituent fixed similar to Theorems I and II may be proved. The theorem is as follows:

THEOREM III. *If l represents the degree of one of the transitive constituents of the subgroup of M composed of all the substitutions leaving a letter of this transitive constituent fixed, or the degree of this subgroup itself when it is transitive, then K must contain a transitive constituent of degree l not in M.*

As in the previous theorems the subgroup K must occur in some conjugate of G_1, as G_1', and when G_1' is considered with respect to the isomorphism which exists between its transitive constituent M' of degree m and the group formed from all the other transitive constituents of G_1', K is seen to occupy in G_1' a place similar to the one which it occupied in G_1. The subgroup of M' which is composed of all the substitutions leaving a letter of M' fixed cannot be entirely the same as that occurring in the transitive constituent M of degree m of G_1. If such were the case, G_1 and G_1' would generate an intransitive group, which is impossible, since G_1 is maximal. If the subgroup of M' leaving a letter fixed is transitive, none of its letters can be the same as those of a corresponding subgroup composed of all the substitutions leaving a letter of the transitive constituent M of G_1 fixed, since each set of l letters is transitively connected. Therefore, K must contain a transitive constituent of degree l which is entirely different from the one appearing in the subgroup of M which is in K. Should the subgroup of M' leaving a letter fixed be intransitive, it will contain certain transitive constituents. At least one of these must be entirely different from any such constituent occurring in the subgroup of M which is in K; otherwise G_1 and G_1' would again generate an intransitive group. Therefore K must again contain a transitive constituent of degree l different entirely from any such constituent occurring in the subgroup of M in G, where l is assumed to represent the degree of any one of the transitive constituents of the subgroup composed of all the substitutions of M which leave a letter fixed.

THEOREM IV. *If G_1 contains a primitive group M_1 of degree m_1 as a transitive constituent, the subgroup of M_1 occurring in K is transitive. Should this transitive subgroup in K also be primitive, G_1 must contain an imprimitive group whose systems of imprimitivity are of degree m_1.*

The subgroup K must occur in some conjugate of G_1, as G_1', and must occupy in G_1' a place similar to the one which it occupied in G_1. Since H is of degree $n - m - 1$ and a primitive group cannot contain an intransitive, invariant subgroup,[*] the subgroup of the transitive constituent of degree m_1 in K must be transitive. The subgroup K must then contain another transitive constituent of degree m_1 similar to the one already in K and which is not a transitive constituent of G_1. If this additional transitive constituent is primitive and is also a part of some transitive constituent of G_1 of degree greater than m_1, it must be a system of imprimitivity of this constituent of larger degree. This follows from the fact that H is of degree $n - m - 1$ and the considered primitive constituent of K of degree m_1 which is a part of a transitive constituent of G_1 has a transitive subgroup in H.

---

[*] Compare Burnside, *Theory of Groups*, p. 187.

COROLLARY I. *If a primitive group of degree m_1 occurs as a factor in G_1, then G_1 must contain an imprimitive group whose systems of imprimitivity are of degree m_1.*

The transitive constituent of degree m_1 occurs as a primitive group in K and, therefore, has a transitive subgroup of degree m_1 in H.

COROLLARY II. *All the transitive constituents of G_1 cannot be primitive groups.*

THEOREM V. *If the transitive constituent M of degree m of G_1 is a primitive group, and if no transitive constituent of degree l occurs in G_1, where l represents the degree of one of the transitive constituents of the subgroup of M leaving a letter fixed, or the degree of this subgroup itself when it is transitive, then when the transitive constituent of degree l of K which is not in M has a transitive subgroup in H, G_1 must contain an imprimitive group of degree ml.*

According to Theorem III the subgroup K must contain a transitive constituent of degree l which is entirely different from any such constituent occurring in the part of K that is in M. Since the order of K is one m-th the order of G_1, this transitive constituent of degree l must be transformed into itself by one m-th the substitutions of G_1. Then since the subgroup composed of all the substitutions of M leaving a letter fixed is a maximal subgroup of a primitive group, if the transitive constituent of degree l in K were transformed into itself by more than one m-th the substitutions of G_1, it would be transformed into itself by the entire G_1. This is impossible, since G_1 is assumed to contain no transitive constituent of degree l. The transitive constituent of degree l in K has a transitive subgroup in H and is not a transitive constituent of G_1; therefore, it must be a system of imprimitivity of some transitive constituent of G_1. Then since the constituent of degree l is transformed into itself by only one m-th the substitutions of G_1, G_1 must contain an imprimitive group of degree ml.

COROLLARY I. *If the transitive constituent of degree l in K which is not in M is a primitive group, G_1 always contains an imprimitive group of degree ml.*

Since H is of degree $n - m - 1$ and an invariant subgroup of a primitive group is transitive, the subgroup of the constituent of degree l in H is always transitive.

COROLLARY II. *If the transitive constituent M of degree m of G_1 is a K-times transitive group, $K \geqq 3$, G_1 always contains an imprimitive group of degree $m(m - 1)$.*

The subgroup composed of all the substitutions leaving a letter of M fixed is at least doubly transitive and, therefore, a primitive group. It is also of degree $m-1$. Therefore, G_1 contains an imprimitive group of degree $m(m-1)$.

THEOREM VI. *If G_1 contains an imprimitive group M of degree m as a transitive constituent, and if no transitive constituent of degree l occurs in G_1, where l represents the degree of any one of the transitive constituents of the subgroup of M composed of all the substitutions leaving a letter of M fixed, then when the transitive constituent of degree l which is not in M has a transitive subgroup in H, G_1 must contain a transitive constituent of degree $m'l$, where m' represents some divisor of m different from* 1.

According to Theorem III the subgroup K of G_1 must contain a transitive constituent of degree l entirely different from any such constituent occurring in the part of K in M. Since the order of K is one m-th the order of G_1, this transitive constituent of degree l must be transformed into itself by at least one m-th the substitutions of G_1. It cannot be transformed into itself by G_1 or G_1 would contain a transitive constituent of degree l. However, the transitive constituent of degree l may be transformed into itself by certain subgroups of G_1 containing K. The orders of such subgroups must then be multiples of the order of K or one m'-th the order of G_1, where m' is some divisor of m different from 1. Then if the transitive constituent of K of degree l is transformed into itself by one m'-th the substitutions of G_1 and the part of the constituent of degree l in H is transitive, it must be a system of imprimitivity of some transitive constituent of G_1, and G_1 must contain a transitive constituent of degree $m'l$.

THEOREM VII. *If G_1 contains a transitive constituent of degree* 3, *it contains another transitive constituent of degree* 3 *or* 6.*

When the transitive constituent of degree 3 is of order 3, the theorem is self-evident, since all the other transitive constituents must be of the same degree and order.† If the constituent of degree 3 is of order 6 and G_1 is of this same order, all the other transitive constituents of G_1 must be of degrees 3 or 6, for only transitive constituents of these degrees can be put in simple isomorphism with the symmetric group of degree 3. It may then be assumed that the order of G_1 is greater than 6, and since the theorem would require no proof if G_1 contained a second transitive constituent of degree 3, it may be assumed that G_1 contains only one transitive constituent of degree 3. Under this assumption H is of degree $n-4$ and Theorem V then states that G_1 must contain a transitive constituent of degree 6.

---

* This theorem was proved by Professor G. A. Miller in a lecture course during the year 1909–10.

† Miller, *Proc. London Math. Soc.*, Vol. XXVIII, p. 536.

THEOREM VIII. *If G_1 contains a group of degree 4 whose order is a power of 2 as a transitive constituent, it must contain another transitive constituent of degree 4 or of degree 8.*

When the transitive constituent of degree 4 is of order 4, G_1 is of order 4 and G is of class $n-1$.* The group of order 8 and degree 4 can be represented only on 4 or 8 letters; therefore, when the transitive constituent of degree 4 is of order 8 and G_1 is of the same order, G_1 can contain only transitive constituents of degrees 4 or 8. Since any transitive constituent in simple isomorphism with the transitive constituent of degree 4 and order 8 must be of degree 4 or 8, it may be assumed that the order of G_1 is greater than 8. The subgroup of the transitive constituent of degree 4 composed of all the substitutions leaving a letter of this constituent of degree 4 fixed is of degree 2. Therefore, K must contain a transitive constituent of degree 2 entirely different from the one occurring in the subgroup composed of all the substitutions leaving a letter of the transitive constituent of degree 4 fixed. Since G_1 cannot contain a transitive constituent of degree 2 and the constituent of degree 2 in K may be transformed into itself by one-fourth and also by one-half of the substitutions of G_1, G_1 must contain a transitive constituent of degree 4 or of degree 8.

THEOREM IX. *If G_1 contains the alternating group of degree 4 as a transitive constituent and the order of G_1 exceeds 12, G_1 must contain a transitive constituent of degree 12 whose order is at least 36.*

When the order of G_1 exceeds 12, there may be an intransitive constituent R of degree r and order 12 formed from the simple isomorphism of certain groups with the considered alternating group of degree 4. The subgroup H will then be of degree $n-r-1$. If such an isomorphism does not occur in G_1, H is of degree $n-5$. In either case K must contain a transitive constituent of degree 3 entirely different from any such constituent occurring in the part of K in the alternating group of degree 4 or in R when it occurs. This constituent of degree 3 is the cyclic group of degree 3. If a constituent of degree 3 occurs in G_1, it must be the symmetric group of degree 3 and occur wholly in H, for G_1 could not contain a constituent of degree 3 and order 3 and

---

[*] Miller, *Bull. Amer. Math. Soc.*, 6 (1899–1900), p. 104.

no isomorphism exists between the symmetric group of degree 3 and the alternating group of degree 4. Therefore, the cyclic constituent of degree 3 cannot be a part of any symmetric constituent of degree 3 that may occur in G_1. Since the additional cyclic group of degree 3 in K must be in H, is transformed into itself by only one-fourth the substitutions of G_1 and could not occur as a transitive constituent of G_1, G_1 must contain a transitive constituent of degree 12. The order of the subgroup of this transitive constituent of degree 12 occurring in H cannot be less than 3. Therefore, G_1 must contain a transitive constituent of degree 12 whose order is at least 36.

THEOREM X. *If* G_1 *contains the symmetric group of degree* 4 *as a transitive constituent and no transitive constituent of degree less than* 4, *then if the order of* G_1 *is* 24, *it must contain another transitive constituent of degree* 4, 6, 8, 12 *or* 24. *If the order of* G_1 *is greater than* 24, *and* H *is of degree* $n - 5$, G_1 *must contain a transitive constituent of degree* 12.

The symmetric group of degree 24 can be represented only on 4, 6, 8, 12, or 24 letters.* Therefore, if the order of G_1 is 24 and no transitive constituent of degree less than 4 occurs, the other transitive constituents, when such occur, can be only of degrees 4, 6, 8, 12, or 24. If the order of G_1 is greater than 24 and H is of degree $n - 5$, from Theorem IV it is evident that a transitive constituent of degree 12 must occur.

PART II.

§ 1. *Simply Transitive Primitive Groups of Degree* 20.

We first observe that the order of a transitive constituent of G_1 and, therefore, the order of G_1 could not be divisible by any one of the primes 5, 7, 11, 13, and 17. If such were the case, G_1 would contain substitutions of these orders† and of degrees $5q$, $7q$, $11q$, $13q$, and $17q$, where q represents the number of cycles in the substitutions of the given orders. When $q = 1$, the degree of the primitive group generated could not exceed $p + 2$,‡ a degree which is less than 20 for each of the primes considered. When $q = 2$, a possibility that occurs for the primes 5 and 7, or when $q = 3$, as is possible for the prime 5, the limit for the degree is again less than 20§ for each of the primitive groups that might be generated. Then since the order of a transitive constituent of G_1 is not divisible by these primes, G_1 could contain no transitive constituent whose degree is divisible by any one of them.* In other words, we see at once that transitive constituents of degrees 17, 15, 13, 11, 10, 7, and 5 cannot occur in G_1. It is also known that G_1 cannot contain a transitive constituent of degree 2. These results together with Theorem VII show immediately that the largest possible degree for any transitive constituent of G_1 is 9.

---

* Dyck, *Math. Ann.*, XXII (1883), pp. 84–86, pp. 105–106.

† Cauchy, *Exercises d' analyse*, 3 (1844), p. 250.

‡ C. Jordan, *Bulletin de la Société Mathématique de France*, Vol. I (1873), pp. 40–71 and pp. 175–221.

§ Manning, *Trans. Amer. Math. Soc.*, Vol. X (1909), p. 252.

We shall first consider all the possible groups when the maximum degree of a transitive constituent of G_1 is 9; then those when this maximum degree is 8, etc.

A transitive constituent of degree 9 cannot occur in G_1. The possible systems of intransitivity which require special consideration are 9, 6, 4 and 9, 4, 3, 3.

When the systems of intransitivity of G_1 are 9, 6, 4 and G_1 is considered with respect to the isomorphism which exists between its transitive constituent of degree 4 and the group formed from the transitive constituents of degrees 9 and 6, it is seen that the order of G_1 must exceed the order of the transitive constituent of degree 4. The subgroup H corresponding to identity in the transitive constituent of degree 4 will be of degree $n - 5$, for the class of G_1 must be at least 12.† Then according to Theorems IX and X, G_1 must contain a transitive constituent of degree 12. This is impossible with the systems of intransitivity 9, 6, 4; therefore, such systems cannot occur in G_1.

When G_1 contains a transitive constituent of prime degree p, the order of G_1 is not divisible by p^2.‡ It is evident, therefore, that the systems of intransitivity 9, 4, 3, 3 cannot occur in G_1.

If G_1 contains a transitive constituent of degree 8, but no transitive constituent of higher degree, its possible systems of intransitivity are 8, 8, 3 and 8, 4, 4, 3. Since only one constituent of degree 3 occurs in either case, Theorem VII shows at once that a transitive constituent of degree 8 cannot occur in G_1.

When G_1 contains a transitive constituent of degree 6, but none of larger degree, the systems of intransitivity of G_1 may be 6, 6, 4, 3 or 6, 4, 3, 3, 3.

---

* Compare Burnside, *Theory of Groups*, p. 140.

† Jordan, C. R., Vol. LXXIII (1871), p. 853; Manning, AMERICAN JOURNAL OF MATHEMATICS, Vol. XXVIII (1906), p. 226.

‡ Rietz, AMERICAN JOURNAL OF MATHEMATICS, Vol. XXVI (1904), p. 6.

It is evident that the transitive constituent of degree 4 must be either the symmetric or the alternating group of this degree and that the constituent of degree 3 must be the symmetric group of degree 3. Since the class of G_1 must be at least 12, in both cases G_1 may be considered as formed from a simple isomorphism between the intransitive group of degree 9 and the intransitive group of degree 10.

If the systems of intransitivity of G_1 are 6, 4, 3, 3, 3, the intransitive group of degree 9 contains only one Sylow subgroup of order 3^a while the intransitive group of degree 10 contains more than one such subgroup. The simple isomorphism, therefore, cannot be established.

If the systems of intransitivity of G_1 are 6, 4, 6, 3, the constituent of degree 6 in the intransitive group of degree 9 must be of order 48, 24, or 12, for the intransitive group of degree 10 has more than one Sylow subgroup of order 3^a. The order of the intransitive group of degree 9 cannot be divisible by 9, for the order of G_1 cannot be divisible by 3^2. The order of G_1 is, therefore, equal to the order of the transitive constituent of degree 6 in the intransitive group of degree 9 or is 48, 24, or 12. It is at once evident that the order of G_1 cannot be 12 since the constituent of degree 3 is the symmetric group of degree 3. The order of G_1 also cannot be 24* and on account of class a G_1 of order 48 cannot be constructed. Therefore, G_1 can contain no transitive constituent of degree 6.

A transitive constituent of degree 4 cannot occur in G_1. The possible systems of intransitivity are 4, 3, 3, 3, 3, 3 and 4, 4, 4, 4, 3. If the systems of intransitivity are 4, 3, 3, 3, 3, 3, G_1 may be considered as formed from a simple isomorphism between an intransitive group of degree 10 and an intransitive group of degree 9. The intransitive group of degree 9 will contain only one Sylow subgroup of order 3^a while the intransitive group of degree 10 contains more than one such subgroup. The considered isomorphism is then impossible. Theorem VI shows at once that the systems of intransitivity 4, 4, 4, 4, 3 cannot occur in G_1.

Since a constituent of degree 2 cannot occur in G_1 and 19 is not divisible by 3, a transitive constituent of degree 3 cannot occur in G_1.

This completes the consideration of the simply transitive primitive groups of degree 20 and shows that no such groups exist.

---

*Miller, *Proc. London Math. Soc.*, Vol. XXVIII, p. 534.

§ 2. *Multiply Transitive Groups of Degree* 20.

A multiply transitive group of degree 20 must have a transitive group of degree 19 as the maximal subgroup composed of all the substitutions leaving a letter fixed. According to the determination made by Jordan, besides the alternating and symmetric groups of degree 19, there are only six transitive groups of this degree, the metacyclic group and its subgroups.* The orders of the latter groups are 19, 2 . 19, 3 . 19, 6 . 19, 9 . 19, and 18 . 19.

Since a transitive group of degree n and order $n(n-1)$ whose operations other than identity displace all, or all but one, of the symbols, can exist only when n is the power of a prime,† no primitive group of degree 20 can have the group of degree and order 19 as a maximal subgroup.

If a primitive group of degree 20 and order 20 . 19 . 2 existed, it would contain both positive and negative substitutions. The subgroup of its positive substitutions would be a group of degree 20 and order 20 . 19. Since such a group has been shown not to exist, the required group of order 20 . 19 . 2 cannot exist.

A primitive group of degree 20 and order 20 . 19 . 3 cannot exist. Such a group must contain

380 substitutions of degree 18, order 3.
360 " " " 19, " 19.
399 " " " 20.

The substitutions of order 5 contained in the group must be of degree 20 having four systems of intransitivity. A subgroup of order 5 cannot be transformed into itself by substitutions of degree 19 nor by substitutions of degree 18 and order 3. Therefore, the number of subgroups of order 5 must be a multiple of 57. From Sylow's theorem the number of subgroups of order 5 must be of the form $5K+1$; there must then be at least 171 subgroups of order 5. Since it is impossible to form 171 subgroups of order 5 from 399 substitutions of degree 20, a primitive group of order 20 . 19 . 3 cannot exist.

A primitive group of degree 20 and order 20 . 19 . 3 . 2 cannot exist. Such a group would be both positive and negative and contain a positive subgroup of order 20 . 19 . 3. Since the positive subgroup does not exist, the group considered cannot exist.

---

* Jordan, C. R., Vol. LXXIX, p. 150.

† Jordan, *Liouville's Journal*, 2^{me} sér., Vol. XVII, p. 355.

Mathieu* has proved that there is at least one triply-transitive group of degree $p+1$ and order $p(p^2-1)$ and one doubly-transitive group of degree $p+1$ and order $\frac{p}{2}(p^2-1)$, p being any prime number. The latter group is composed of the positive substitutions of the former. Frobenius has further proved that there is only one group of each order except for the case $p=7$ when there are two groups of order $\frac{p}{2}(p^2-1)$.† For degree 20 there is then only one primitive group of order $20 \,.\, 19 \,.\, 9$ and only one primitive group of order $20 \,.\, 19 \,.\, 18$.

This completes the determination of the primitive groups of degree 20. Besides the symmetric and alternating groups of this degree, there are only two primitive groups and these are the well-known Mathieu groups of orders $p(p^2-1)$ and $\frac{p}{2}(p^2-1)$.

PART III.

Certain Primitive Groups whose Maximal Subgroup Contains a Transitive Constituent of Prime Order.

In the following discussion G will be considered as denoting any primitive group of degree n whose maximal subgroup contains a transitive constituent of order p, p an odd prime. We first observe that G_1 must be of order p and G of class $n-1$.‡ Then according to Frobenius, the degree of G is of form q^a, q a prime, and G contains a characteristic abelian subgroup H of degree q^a and type $(1, 1, \ldots, 1)$.§

THEOREM 1. *If the number of transitive constituents of prime order* p *of* G_1 *is* 2^α, $\alpha > 0$, *the degree of* G *is of form* $2^\alpha p + 1 = q^a$, q *an odd prime. If* a *is even, a primitive group* G *can exist only when* $a \equiv 0$, *mod.* 4, *or when* $a = 2$ *and* q *belongs to exponent* 2, *mod.* p, *and there is only one group* G *for each set of values of* p *and* α *for which the equation* $2^\alpha p + 1 = q^2$ *is satisfied. If* a *is odd, the group* G *can exist only when* a *is* 1 *or a prime. When* $a = 1$, G *is a subgroup of the metacyclic group. In case* $a \neq 1$ *and odd,* α *can be only* 1 *or some power of* 2, *as* 2^γ. *When* $a \neq 1$ *and* $\alpha = 1$, *there is one and only one primitive group* G *of degree* 3^a *for*

---

* Mathieu, *Journal de Mathématiques*, Vol. V (1860), p. 37.

† Frobenius, *Berliner Sitzungsberichte* (1902), pp. 455–459.

‡ Miller, *Proc. London Math. Soc.*, Vol. XXVIII, p. 536.

§ Frobenius, *Berliner Sitzungsberichte* (1902), pp. 455–59.

each prime p for which $2p + 1 = 3^a$. *When* $a \neq 1$ *and* $\alpha = 2^{\gamma}$, *one and only one primitive group G exists for each set of values of p and* γ *for which* $2^{2^{\gamma}}p + 1 = q^a$.

Since G_1 contains 2^{α} transitive constituents of order p, the degree of G_1 is $2^{\alpha}p$ and the degree of G is $2^{\alpha}p + 1$, an odd number. But the degree of G must be the power of a prime; therefore,

$$2^{\alpha}p + 1 = q^a, \tag{I}$$

q an odd prime. It will now be shown that Equation (I) can exist, if a is even, only when $a = 2$ or $a \equiv 0$, mod. 4. We have, when a is even,

$$2^{\alpha}p = q^a - 1 = (q-1)(q+1)(q^{a-2} + q^{a-4} + \dots + 1) = (q-1)(q+1)K.$$

If $a > 2$ and $\not\equiv 0$, mod. 4, K must be odd and, therefore, $K = p$ and $2^{\alpha} = q^2 - 1$. The latter equation is satisfied only when $\alpha = 3$ and $q = 3$. Equation (I) then becomes $8p + 1 = 3^a$, an equation which does not exist under the given conditions. Therefore, Equation (I) cannot exist when a is even, greater than 2 and $\not\equiv 0$, mod. 4.

If $2^{\alpha}p + 1 = q^2$, q must belong to exponent 2, mod. p, or exponent 1, mod. p. Suppose q belongs to exponent 2, mod. p. The order of the group of isomorphisms of the abelian group of order q^2 is divisible by p while $q^2 - 1$ is not divisible by p^x, $x > 1$. Then for each set of values of p and α only one primitive group G can exist for $a = 2$.* The primitive group of order 75 and degree 25 is an example of this type of group. Here $\alpha = 3$, $p = 3$, and $q = 5$.

When q belongs to exponent 1, mod. p, the number of subgroups of order q is not divisible by p. The subgroup G_1 is then not maximal and G is not primitive.

Now consider that a is odd and first assume that $a = mn$, m and n odd primes. Then

$$2^{\alpha}p = q^{mn} - 1 = (q-1)(q^{m-1} + q^{m-2} + \dots + 1)[(q^m)^{n-1} + (q^m)^{n-2} + \dots + 1],$$

which is at once seen to be impossible unless either m or n is 1 or both m and n are 1. Thus a must be 1 or a prime.

When $a = 1$, we have $2^{\alpha}p + 1 = q$ and G is a subgroup of the metacyclic group. There is only one such group for each set of values of p and α for which the equation $2^{\alpha}p + 1 = q$ is satisfied.

---

* Rietz, AMERICAN JOURNAL, Vol. XXVI (1904), p. 12.

When a is an odd prime, $2^\alpha = q - 1$ or $q = 2^\alpha + 1$. Assume that α is odd. Then we have

$$q = 2^\alpha + 1 = (2 + 1)(2^{\alpha-1} - 2^{\alpha-2} + \ldots . + 1).$$

Therefore $\alpha = 1$ when odd and $q = 3$. Assume that α is even and that $\alpha = Kl$, where K consists of powers of 2 and l consists of odd factors only. Then

$$q = 2^\alpha + 1 = 2^{kl} + 1 = (2^k + 1)[(2^k)^{l-1} - \ldots . + 1].$$

Therefore, $l = 1$ and $\alpha = 2^\gamma$ when α is even.

When a is an odd prime and $\alpha = 1$, we have $2p + 1 = 3^a$ and G is of class $2p$. Since all the groups of class $2p$ have been determined,* it is known at once that this condition gives a primitive group G of degree 3^a for each prime p for which $2p + 1 = 3^a$.

When a is an odd prime and $\alpha = 2^\gamma$, we have

$$2^{2^\gamma} p = q^a - 1 = (q - 1)(q^{a-1} + q^{a-2} + \ldots . + 1)$$

or

$$q - 1 = 2^{2^\gamma} \text{ and } p = q^{a-1} + q^{a-2} + \ldots . + 1.$$

Therefore, if the equation $2^{2^\gamma} p + 1 = q^a$ is satisfied, a is the exponent to which q belongs, mod. p. The order of the group of isomorphisms of the abelian group of order q^a is divisible by p and $q^a - 1$ is not divisible by p^x, $x > 1$. Then there is one and only one group G for each set of values of p and α for which $2^{2^\gamma} + 1 = q^a$.† The primitive group of degree 125 and order 125 . 31 is an example of the above type of group.

THEOREM II. *If the number of transitive constituents of prime order p is an odd prime r, then a primitive group G may only exist when its degree is of form $rp + 1 = 2^a$, where a is 4, an odd prime, or the square of an odd prime. There is only one primitive group G when $a = 4$. If $a = \beta^2$, β an odd prime, for each set of values of r and p for which the equation $rp + 1 = 2^{\beta^2}$ exists only one primitive group G occurs. If a is an odd prime β, for each set of values of r and p for which the equations $rp + 1 = 2^\beta$ exists, $r \neq p$, two primitive groups always occur.*

Since G_1 contains r transitive constituents of prime order p, the degree of G_1 will be represented by rp and the degree of G by the expression $rp + 1$. But $rp + 1$ is even and the degree of G must be the power of a prime; therefore,

$$rp + 1 = 2^a. \qquad \text{(I)}$$

---

* Manning, *Trans. Amer. Math. Soc.*, Vol. IV, pp. 351–57.

† Rietz, AMERICAN JOURNAL OF MATHEMATICS, Vol. XXVI (1904), p. 12.

It is first assumed that a is even. If $a \equiv 2$, mod. 4, we have

$$rp = 2^a - 1 = 2^{2\beta} - 1 = (2^{\beta-1} + \dots + 1) \,.\, 3 \,.\, (2^{\beta-1} - 2^{\beta-2} + \dots + 1);$$

that is, rp would have at least three factors unless $\beta = 1$ when it has only one. Both conditions are impossible.

If $a \equiv 0$, mod. 4, we have

$$rp = 2^a - 1 = 2^{4\beta} - 1 = (2^\beta - 1)(2^\beta + 1)(2^{2\beta} + 1),$$

which has three factors unless $\beta = 1$. When $\beta = 1$ and $p = 5$, a primitive group of degree 16 and order 80 exists. The group is not primitive, if $p = 3$.

Now assume that a is odd. The exponent a may be the product of like or unlike odd primes or a prime.

If $a = \beta\gamma$, β an odd prime and γ one or more old primes, $\beta < \gamma$,

$$rq = 2^{\beta\gamma} - 1 = (2^\beta - 1)[(2^\beta)^{\gamma-1} + (2^\beta)^{\gamma-2} + \dots + 2^\beta + 1] = L \,.\, M, \quad \text{(II)}$$

$$rq = (2^\gamma)^\beta - 1 = (2^\gamma - 1)[(2^\gamma)^{\beta-1} + (2^\gamma)^{\beta-2} + \dots + 2^\gamma + 1] = S \,.\, T. \quad \text{(III)}$$

If L is not a prime, (II) contains too many prime factors. If L is a prime, it must divide either S or T and rq is again equal to more than two prime factors, which is impossible. Therefore, $a \neq \beta\gamma$. If $\beta = \gamma$ or $\gamma = 1$, that is, $a = \beta^2$ or $a = \beta$, it is evident that (I) may exist: Then if a is odd, it must be the square of a prime or a prime.

Assume that $\beta = \gamma$, that is, $a = \beta^2$. Then

$$rp = 2^{\beta^2} - 1 = (2^\beta - 1)[(2^\beta)^{\beta-1} + (2^\beta)^{\beta-2} + \dots + 1].$$

If $r < p$ and the equation $rp + 1 = 2^{\beta^2}$ exists,

$$r = 2^\beta - 1 \quad \text{and} \quad p = (2^\beta)^{\beta-1} + \dots + 2^\beta + 1.$$

In this case 2 belongs to exponent β, mod. r, and exponent β^2, mod. p.

When β^2 is the exponent to which 2 belongs, mod. p, the group G whose G_1 contains r systems of order p is primitive. Only one such group can exist for each prime p. The order of the holomorph L of the abelian group of order 2^{β^2} is $(2^{\beta^2} - 1)(2^{\beta^2} - 2) \dots (2^{\beta^2} - 2^{\beta^2-1}) \,.\, 2^{\beta^2}$. This is divisible by p, but not by p^2. Then all the subgroups of order p in L are conjugate and, therefore, all subgroups of order $2^{\beta^2}p$ are also conjugate. There is then for each set of values of r and p, $r < p$, only the one primitive group whose G_1 contains systems of order p. Such a primitive group occurs when $r = 7$, $p = 73$, and $\beta^2 = 9$.

If $p < r$, $p = 2^\beta - 1$ and $r = (2^\beta)^{\beta-1} + \ldots\ldots + 2^\beta + 1$. Then 2 belongs to exponent β, mod. p. In this case there is no primitive group G containing r systems of order p in its G_1. The number of subgroups of order 2^β occurring in the abelian group H of order 2^{β^2} is

$$\frac{(2^{\beta^2} - 1)(2^{\beta^2-1} - 1)\ldots\ldots(2^{\beta^2-(\beta-1)} - 1)}{(2 - 1)(2^2 - 1)\ldots\ldots(2^\beta - 1)} = N.$$

But N is not divisible by p. Then some subgroups of H of order 2^β are invariant under p or G_1 is not maximal and a primitive group G does not exist. Therefore, for each set of values of r and p for which the equation $rp + 1 = 2^{\beta^2}$ exists, only one primitive group G occurs.

Now assume that $\gamma = 1$, that is, $a = \beta$. Then $rp + 1 = 2^\beta$, β an odd prime, and β is the exponent to which 2 belongs, mod. r, and also mod. p. The order of the holomorph of the abelian group H of order 2^β is divisible by p and r, but by no higher powers of these primes. Then it may be shown as in the previous cases that there exists a primitive group G containing r systems of order p. However, if the equation $rp + 1 = 2^\beta$ exists, this existence is not destroyed if r and p exchange values. Suppose this change is effected. Then since 2 belongs to exponent β, mod. r, it will also belong to exponent β, mod. p, where p has the value previously held by r. For this latter condition by processes similar to those already used, it may be shown that another primitive group G of degree 2^β exists. Therefore, for each set of values of r and p, $r \neq p$, for which the equation $rp + 1 = 2^\beta$ exists, two primitive groups always occur. Two such primitive groups exist, for instance, for the relation $23 \,.\, 89 = 2^{11} - 1$. Both are of degree 2^{11}, but the G_1 of one contains 23 transitive constituents of order 89, while the G_1 of the other contains 89 transitive constituents of order 23.

THEOREM III. *If the number of transitive constituents of prime order* p *occurring in* G_1 *is* $2r$, r *an odd prime, then a primitive group* G *can only exist when the degree is of form* $2rp + 1 = q^a$, *where* q *is a prime of form* $4n + 3$ *and* a *is* 1, *an odd prime, or the square of an odd prime. If* $a = 1$, *the group* G *is a subgroup of the metacyclic group. If* $a = \beta^2$, β *an odd prime, the degree of* G *is of form* 3^{β^2} *and for each set of values of* r *and* p *for which the equation* $2rp + 1 = 3^{\beta^2}$ *exists, only one primitive group* G *occurs. If* $a = \beta$ *and* $q \neq 3$ *for each set of values of* r *and* p *for which the equation* $2rp + 1 = q^\beta$ *exists, only one primitive group* G *is possible, while if* $a = \beta$ *and* $q = 3$, $r \neq p$, *two groups are possible.*

Since the number of transitive constituents of prime order p in G_1 is $2r$, the degree of G may be represented by $2rp+1$. But the degree of G must also be the power of a prime; therefore, we have

$$2rp + 1 = q^{\alpha}, \tag{I}$$

q an odd prime.

The left-hand member of this expression is always congruent to 3, mod. 4, whatever values p and r may have. Therefore, q must be a prime of form $4n+3$ and α an odd number.

Consider $2rp = q^{\beta\gamma} - 1$, where $\alpha = \beta\gamma$, β being an odd prime and γ one or more odd primes, $\beta < \gamma$,

$$\begin{aligned} 2rp = q^{\beta\gamma} - 1 &= (q-1)(q^{\beta-1} + \ldots\ldots + 1)[(q^{\beta})^{\gamma-1} + (q^{\beta})^{\gamma-2} + \ldots\ldots + 1] \\ &= (q-1)L \,.\, R, \end{aligned} \tag{II}$$

$$\begin{aligned} 2rp = q^{\beta\gamma} - 1 &= (q-1)(q^{\gamma-1} + \ldots\ldots + 1)[(q^{\gamma})^{\beta-1} + (q^{\gamma})^{\beta-2} + \ldots\ldots + 1] \\ &= (q-1)M.\,N. \end{aligned} \tag{III}$$

It is evident that Equations (II) and (III) can exist only if $q = 3$. Then if L in (II) is not a prime, $q^{\beta\gamma} - 1$ has too many prime factors. If L is a prime, it must divide either M or N since it is different from both and a number can be resolved into its prime factors in only one way. Again $q^{\beta\gamma} - 1$ has more than two odd prime factors. Therefore, (I) cannot exist when $\alpha = \beta\gamma$.

An inspection of Equations (II) and (III) shows that the existence of the equation $2rp = q^{\alpha} - 1$ may be considered possible if $\beta = \gamma = 1$, $\beta = \gamma$, or $\gamma = 1$, that is, $\alpha = 1$, $\alpha = \beta^2$, or $\alpha = \beta$.

When $\alpha = 1$, $2rp + 1 = q$ and G is a subgroup of the metacyclic group.

When $\gamma = \beta$, we have

$$2rp = q^{\beta^2} - 1 = (q-1)(q^{\beta-1} + q^{\beta-2} + \ldots\ldots + 1)[(q^{\beta})^{\beta-1} + \ldots\ldots + 1].$$

In order that $q^{\beta^2} - 1$ may not contain too many prime factors, q must be 3. Assume $r < p$. Then

$$r = 3^{\beta-1} + 3^{\beta-2} + \ldots\ldots + 1$$

and

$$p = (3^{\beta})^{\beta-1} + (3^{\beta})^{\beta-2} + \ldots\ldots + 3^{\beta} + 1.$$

These values for r and p show that 3 belongs to exponent β^2, mod. p, and exponent β, mod. r. Since β^2 is the exponent to which 3 belongs, mod. p, a primitive group G exists. Also since the order of the group of isomorphisms of the abelian group H of order 3^{β^2} is divisible by p and $3^{\beta^2} - 1$ is not divisible by p^x, $x > 1$, only one such group G exists for each set of values of r and p for which the equation $2rp + 1 = 3^{\beta^2}$ is satisfied.

Assume $r > p$. Then $p = 3^{\beta-1} + 3^{\beta-2} + \ldots\ldots + 1$ and 3 belongs to exponent β, mod. p. In this case no primitive group G exists. For the number of subgroups of order 3^β in the abelian group H of order 3 is not divisible by p. Then G_1 is not maximal and there can be no primitive group G for $r > p$.

If $p = 757$, $r = 13$, and $\beta = 3$, a group G illustrating the case when $r < p$ occurs.

When $\gamma = 1$ and $q \neq 3$, we have $a = \beta$ and

$$2rp = q^\beta - 1 = (q - 1)(q^{\beta-1} + q^{\beta-2} + \ldots\ldots + q + 1).$$

If $r < p$, $2r = q - 1$ and $p = q^{\beta-1} + q^{\beta-2} + \ldots\ldots + 1$. Then q belongs to exponent 1, mod. r, and exponent β, mod. p. As in the previous cases, it may be shown that one and only one primitive group G occurs for each set of values of r and p for which the equation $2rp + 1 = q^\beta$ exists. As an illustration, this equation is satisfied when $\beta = 5$, $q = 7$, $r = 3$, and $p = 2801$ and a primitive group G exists whose G_1 contains 6 transitive constituents of order 2801.

If $r > p$, there is no primitive group G existing. Then $p = \frac{q-1}{2}$ and the number of subgroups of order q in the abelian group H of order q^β is not divisible by p and G_1 is not maximal.

When $q = 3$ and $\gamma = 1$, $a = \beta$ and

$$2rp = 3^\beta - 1 = 2(3^{\beta-1} + 3^{\beta-1} + \ldots\ldots + 3 + 1)$$

or

$$rp = 3^{\beta-1} + 3^{\beta-2} + \ldots\ldots + 3 + 1 = S\,.\,T.$$

Assume $S \neq T$. If $p = T$, and again when $p = S$, 3 belongs to exponent β, mod. p. Also for both values of p the order of the group of isomorphisms of the abelian group H of order 3^β is divisible by p and $3^\beta - 1$ is not divisible by p^2. Then for each of these values of p, one and only one primitive group G exists. Therefore, if $a = \beta$ and $q = 3$ for each set of values of r and p, $r \neq p$, for which the equation $2rp + 1 = 3^\beta$ is satisfied, two primitive groups exist. The identity $2 \,.\, 23 \,.\, 3851 = 3^{11} - 1$ gives one set of values of r and p for which two primitive groups exist.

THEOREM IV. *If the number of transitive constituents of prime order p of G_1 is rq, r and q odd primes, the degree of G is of form $rqp + 1 = 2^a$. Then if 2 belongs to an even exponent with respect to any one of the primes r, q, and p,* *a primitive group G can exist only when its degree is 2^8 or 2^{2b}, b an odd prime. If $a = 8$, only one primitive group G exists. If $a = 2b$, b an odd prime, for each set of values of r, q, and p for which the equation $rqp + 1 = 2^{2b}$ is satisfied, only one primitive group G is possible.*

Since G_1 contains rq transitive constituents of order p, the degree of G_1 is rqp and the degree of G is $rqp + 1$, an even number. But the degree of G is also the power of a prime; therefore,

$$rqp + 1 = 2^a.$$

If 2 belongs to an even exponent with respect to any one of the primes r, q, and p, a must be even. Consider $a \equiv 2$, mod. 4, and assume $a = 2bc$, b an odd prime and c the other odd factors, if such exist. Then

$$\begin{aligned} rqp = 2^{2bc} - 1 = (2^b - 1)[(2^b)^{c-1} + (2^b)^{c-2} + \cdots\cdots + 1] \\ (2^b + 1)[(2^b)^{c-1} - \cdots\cdots + 1]. \end{aligned}$$

This equation is evidently impossible unless $c = 1$. It then becomes

$$rqp = (2^b - 1) . 3 . (2^{b-1} - 2^{b-2} + \cdots\cdots + 1).$$

Therefore, when $a \equiv 2$, mod. 4, $a = 2b$, b an odd prime. Let

$$p = (2^{b-1} - 2^{b-2} + \cdots\cdots + 1).$$

Then 2 belongs to exponent $2b$, mod. p, and by considering the holomorph of the abelian group of order 2^{2b}, it may be shown by methods similar to those used in Theorem II that for this value of p only one primitive group G exists. If p were equal to either one of the other factors of $2^{2b} - 1$, no primitive group G could exist. Therefore, for each set of values of r, q, and p for which the equation $rqp + 1 = 2^a$ is satisfied, only one primitive group G exists. Such a primitive group occurs when $rq = 9$ and $p = 7$, also when $rq = 93$ and $p = 11$.

Now consider that $a \equiv 0$, mod. 4, and assume $a = 4c$. Then we must have

$$rqp = 2^{4c} - 1 = (2^c - 1)(2^c + 1)(2^{2c} + 1).$$

If $c = 1$, the above equation is impossible; and if $c > 1$ and odd, it is also impossible. Therefore, c must be even, or $a = 8d$ and

$$rqp = 2^{8d} - 1 = (2^d - 1)(2^d + 1)(2^{2d} + 1)(2^{4d} + 1).$$

In order that the above equation may exist, d must be 1. Therefore, if $a \equiv 0$, mod. 4, $a = 8$. When $a = 8$, $rq = 15$ and $p = 17$ and only one primitive group G exists.

UNIVERSITY OF ILLINOIS, *June*, 1910.